EXHIBIT H

Musk's DOGE agents access sensitive personnel data, alarming security officials

The highly restricted data includes personally identifiable information for millions of federal employees maintained by the Office of Personnel Management.

February 6, 2025

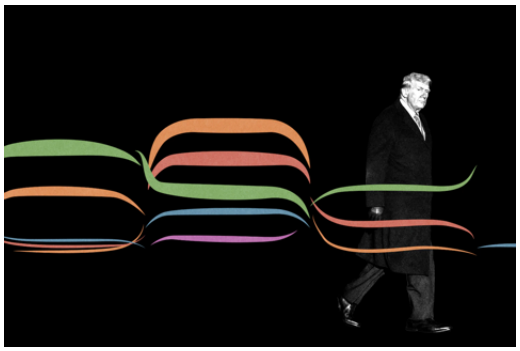
By Isaac Stanley-Becker, Greg Miller, Hannah Natanson and Joseph Menn

Agents of billionaire Elon Musk's Department of Government Efficiency have gained access to highly restricted government records on millions of federal employees — including Treasury and State Department officials in sensitive security positions — as part of a broader effort to take control over the government's main personnel agency, according to four U.S. officials with knowledge of the developments.

The officials, who like others spoke on the condition of anonymity for fear of reprisal, expressed alarm about potential breaches or abuses of such records by members of an administration whose senior-most officials, including President Donald Trump, have threatened to retaliate against federal workers accused of disloyalty.

Trump presidency

Follow live updates on the Trump administration. We're tracking Trump's progress on campaign promises and legal challenges to his executive orders and actions.



The records maintained by the Office of Personnel Management, or OPM, amount to a repository of sensitive information about employees of most federal agencies — including addresses, demographic profiles, salary details and disciplinary histories. The moves at the OPM by members of Musk's pseudo-governmental DOGE have coincided with similar efforts to gain access to sensitive systems at other agencies, including a Treasury Department system responsible for processing trillions of dollars in U.S. government payments — a development reported last week by The Washington Post.

Records obtained by The Post show that several members of Musk's DOGE team — some of whom are in their early 20s and come from positions at his private companies — were given "administrative" access to OPM computer systems within days of Trump's inauguration last month. That gives them sweeping authority to install and modify software on government-supplied equipment and, according to two OPM officials, to alter internal documentation of their own activities.

The DOGE team's demand for access to OPM files and networks came as Musk deputies arrived at the agency promising to wipe out 70 percent of its staff, officials said. A senior OPM official, during a team meeting Wednesday, said that core units focused on modernizing the agency's network and improving accountability are "likely to go away," according to a recording of the session obtained by The Post. Those who have been reassigned at the agency include the chief information officer and the chief financial officer.

Meanwhile, morale has plummeted, said three OPM officials, as DOGE agents have clashed with senior career personnel. One official recalled a recent meeting in which a young DOGE team member began screaming at senior developers and calling them "idiots."

A halt to IT upgrades — along with fresh access by outsiders with the power to install new programs — could create novel vulnerabilities at an agency that has been repeatedly hacked by foreign intelligence services. The worst came in 2014, when China is believed to have obtained the background investigations of more than 20 million people seeking security clearances.

“It’s like you’re defending some medieval castle and someone comes in and starts firing all the archers who are positioned to defend it,” a former U.S. intelligence official said. “You let your defenses down. It’s a perfect time to strike.”

A DOGE representative did not address questions about data access and other permissions. Emailed questions to the OPM went unanswered. A U.S. official maintained that everyone with access to sensitive systems is a government employee with the appropriate clearances.

The Trump administration has suggested that members of the DOGE team have the authority to review sensitive government files but has refused to provide details about whether security clearances have been issued. The speed with which any clearances would have been supplied suggests they may have skipped customary precautions, including FBI background checks, U.S. officials said.

Trump issued an executive order last month that bypasses the normal procedure for White House staff security checks, though DOGE went unmentioned.

At least six DOGE agents were given broad access to all personnel systems at the OPM on the afternoon of Jan. 20, the day of Trump’s inauguration, according to two agency officials. Three more gained access about a week later, they said.

The data that the DOGE team can access includes a massive trove of personal information for millions of federal employees, included in systems called Enterprise Human Resources Integration and Electronic Official Personnel Folder. It also includes personal information for anyone who applied to a federal job through the site USAJobs, the people said. Last year alone, the people said, there were 24.5 million such applicants.

The two OPM officials said the level of access granted to DOGE agents means they could copy the Social Security numbers, phone numbers and personnel files for millions of federal employees.

“They could put a new file in someone’s record; they could modify an existing record,” one said. “They could delete that record out of the database. They could export all that data about people who are currently or formerly employed by the government, they could export it to some nongovernment server, or to their own PC, or to a Google Drive. Or to a foreign country.”

None of the officials said they had witnessed DOGE representatives engaging in such conduct but were nonetheless disturbed by the scope of the data now under their control. The OPM’s new leadership argued in a court filing Wednesday that access to personnel databases was used simply to create a government-wide email system.

But the aggregate information contained in the OPM databases is so sensitive, said a U.S. official, that even White House requests for certain types of data were rebuffed under previous administrations. The official said those controls exist to "make sure that data is used in a way that protects the individuals."

The disruptions at the OPM, Treasury and other agencies have raised concerns among U.S. security officials and experts that Russia, China, Iran and other adversaries could seek to exploit the chaos by launching new cyber intrusions or targeting the devices and communications of Musk's team.

A former U.S. security official said DOGE's access to Treasury's payment system is alarming, describing it as a comprehensive map to U.S. expenditures encompassing highly classified programs and purposes. The agency said this week that Musk's agents have "read-only access."

Funding "for everything the U.S. government does from food stamps to paying assets [overseas] originates at Treasury," the former security official said. "We have a whole bunch of classified relationships with U.S. businesses" under contract with U.S. intelligence agencies. The payment system "is a road map" to U.S. secrets coveted by foreign intelligence services.

Marcus Hutchins, a cybersecurity expert who stopped the 2017 WannaCry ransomware worm attributed to North Korea, said the risks would multiply with every new user and new machine plugged in at OPM.

"It's highly likely they're improperly accessing, transferring and storing highly sensitive data outside of the environments it was intended to be contained within," he said. "If I were a nation like China, Russia or Iran, I'd be having a field day with a bunch of college kids running around with sensitive federal government data on unencrypted hard drives."

Democratic members of the Senate Intelligence Committee wrote a letter Wednesday to White House Chief of Staff Susie Wiles demanding that the administration provide details to Congress about how DOGE agents are being vetted and what sensitive systems they are handling.

Devastating data breaches a decade ago intensified security protocols at the OPM, which no longer holds CIA background checks, for instance. The agency traditionally allows access to sensitive personnel data to a select number of career officials, allowing others to review it on a need-to-know basis, according to current and former U.S. officials.

A class-action lawsuit filed against the OPM in late January alleges that the agency violated federal privacy laws when rolling out the new communication system enabling email blasts to all federal employees.

"Secure communications take time and coordination to plan and implement," says the lawsuit, filed by Kelly B. McClanahan, executive director of National Security Counselors, a public interest law firm. "Standard email is not encrypted, and it is common practice among hackers — including hackers affiliated with hostile foreign services — to begin attempting to access a new U.S. Government device as soon as they learn of its deployment."

In response, the OPM maintained in a filing that a "privacy impact assessment" was not required but submitted one anyway. The assessment, dated Wednesday, confirms that the new government-wide email system is drawn from the restricted databases but asserts that its use is simply to gather names, email addresses and voluntary responses to the offer of deferred resignation. The assessment indicates that the new email system "operates entirely on government computers" and maintains that information is accessed only "by a handful of individuals within OPM."

Wednesday's privacy assessment identifies the agency's point of contact as Riccardo Biasini, previously an employee at a Musk firm called the Boring Company. The assessment notes that OPM employees are required to take security training on an annual basis. But the new chief information officer, Greg Hogan, who is vested with authority over the new government-wide email system, was installed in his role just last month.

A former senior U.S. security official said foreign adversaries see the disruption caused by DOGE as an opportunity.

"If I were the Russians or Chinese or Iranians and I saw this DOGE operation getting formed, I would be seeding people into this operation like crazy," the former official said. "Either people they've already seeded into these companies or people they can recruit quickly and put forward. I can't believe the DOGE operation was itself carefully vetting everybody prepared to work for it."

Miller reported from London and Menn from San Francisco. Alice Crites, Emily Davies, Ellen Nakashima, Razzan Nakhlawi and Aaron Schaffer contributed to this report.

What readers are saying

The comments express significant concern over the potential security risks posed by the DOGE team's access to sensitive government data. Many commenters view this situation as a severe breach of privacy and national security, likening it to a coup or hostile takeover. There is a... Show more

This summary is AI-generated. AI can make mistakes and this summary is not a replacement for reading the comments.